## IN THE DRAWINGS

A set of formal drawings FIGURES 1 through 8, is attached to this Preliminary Amendment.

## IN THE CLAIMS

Cancel Claims 1 through 12 originally filed with this application in both the German language copy and in the certified English translation.

Add new Claims 13 through 34 as follows herein.

13. A procedure for the protection of computer software and/or computer-readable data against unauthorized use, including the steps of:

encoding of software or data by a licenser dependent on license parameters containing a Firm Code (FC) assigned to said licenser and a User Code (UC) allocated by said licenser of the software or the data, which together initiate the encoding;

storing the encoded software or data on a data medium of a licensee;

sending an encoded transmission of the license parameters from said licenser to said licensee;

storing the license parameters in a nonvolatile memory of said licensee;

automatically decoding the software or data by means of a decoder dependent on the storage license parameters during the use of the software or data by said licensee wherein:

encoding of software or data is initialized dependent on a secret Firm Key (FK) freely selected by said licenser;

the encoding of the transmission of the license parameters occurs dependent on a secret Private Serial Key (SK); and

the decoding of the software or data is initialized dependent on the Firm Key (FK) selected by said licenser.

14. A procedure in accordance with Claim 13, wherein:

the secret Private Serial Key (SK) is produced randomly at said licensee without said licensee, said licenser, or anyone else being able to influence that.

15. A procedure in accordance with Claim 13, wherein:

the signature of the transmission of the license parameters from said licenser to said licensee occurs dependent on a unique Serial Number (SN) firmly assigned to said licensee.

16.   A procedure in accordance with Claim 13 wherein:

said licenser is assigned a secret Firm Common Key (FCK), which is produced from a Common Key (CK) through encoding dependent on the Firm Code (FC) of said licenser; and

the installation, changing, or deletion of the license parameters occurs dependent on the Firm Common Key (FCK).

17.   A procedure in accordance with Claim 13 wherein:

the storage of the license parameters occurs within a protective device developed as a hardware supplement.

18.   A procedure in accordance with Claim 17 wherein:

the automatic decoding of the protected software or data occurs by means of an encoder and decoder arranged within the protective device.

19.   A procedure in accordance with Claim 17 wherein:

the protective device contains a limiter secure against manipulation that limits the time period and/or the number of decodings of the protected software or data.

20.   A procedure in accordance with Claim 17 wherein:

a secret Private Box Key (BK) determined by a producer is stored in the protective device; and

the encoding of the transmission of license parameters between said licenser and the licensee occurs dependent on this Private Box Key (BK).

21. A protective device for use in a procedure in accordance with Claim 13, comprising:

an interface for connection with a computer of said licensee;

a microprocessor;

a nonvolatile memory in which the license parameters are stored; and

an encoder and decoder for the automatic decoding of the software or data dependent on the stored license parameters; and

an installation for the production of a random secret Private Serial Key (SK) for the encoding of the transmission of the license parameters between said licenser and said licensee.

22. A protective device in accordance with Claim 21, wherein:

the memory includes several memory areas for the storage of license parameters of different licensers.

23. A protective device in accordance with Claim 21 wherein:

the microprocessor, the memory, the encoder/ decoder, and the installation for the production of the Private Serial Key (SK) are developed on a single integrated semiconductor circuit (ASIC).

24. A protective device in accordance with Claim 21 including:

a limiter secure from manipulation that limits the time period and/or the number of decodings of the protected software or data.

17

25. A procedure for the protection of computer software and/or computer-readable data against unauthorized use, including the steps of:

encoding of software or data by a licenser dependent on license parameters containing a Firm Code (FC) assigned to said licenser and a User Code (UC) allocated by said licenser of the software or the data, which together initiate the encoding;

storing the encoded software or data on a data medium of a licensee;

sending an encoded transmission of the license parameters from said licenser to said licensee;

automatically decoding the software or data by means of a decoder dependent on the license parameters during the use of the software or data by said licensee;

initializing encoding of software or data dependent on a secret Firm Key (FK) freely selected by said licenser;

encoding of the transmission of the license parameters dependent on a secret Private Serial Key (SK);

initializing decoding of the software or data dependent on the Firm Key (FK) selected by said licenser;

producing the secret Private Serial Key (SK) randomly at said licensee; and

storing the license parameters within a memory of a protective device.

26. A procedure in accordance with Claim 25, wherein:

the signature of the transmission of the license parameters from said licenser to said licensee occurs dependent on a unique Serial Number (SN) firmly assigned to said licensee.

27. A procedure in accordance with Claim 25 wherein:

said licenser is assigned a secret Firm Common Key (FCK), which is produced from a Common Key (CK) through encoding dependent on the Firm Code (FC) of said licenser; and

the installation, changing, or deletion of the license parameters occurs dependent on the Firm Common Key (FCK).

28. A procedure in accordance with Claim 25 wherein:

the automatic decoding of the protected software or data occurs by means of an encoder and decoder arranged within the protective device.

29. A procedure in accordance with Claim 25 wherein:

the protective device contains a limiter secure against manipulation that limits the time period and/or the number of decodings of the protected software or data.

30. A procedure in accordance with Claim 25 wherein:

a secret Private Box Key (BK) determined by a producer is stored in the protective device; and

the encoding of the transmission of license parameters between said licenser and the licensee occurs dependent on this Private Box Key (BK).

31. A protective device for use in a procedure which includes encoding of software or data by a licenser dependent on license parameters containing a Firm Code (FC) assigned to said licenser and a User Code (UC) allocated by said licenser of the software or the data, which together initiate the encoding;

storing the encoded software or data on a data medium of a licensee;

sending an encoded transmission of the license parameters from said licenser to said licensee;

automatically decoding the software or data by means of a decoder dependent on the license parameters during the use of the software or data by said licensee;

initializing encoding of software or data dependent on a secret Firm Key (FK) freely selected by said licenser;

encoding the transmission of the license parameters dependent on a secret Private Serial Key (SK); and

initializing the decoding of the software or data dependent on the Firm Key (FK) selected by said licenser, said protective device comprising:

an interface for connection with a computer of said licensee;

a microprocessor;

a nonvolatile memory in which the license parameters are stored;

an encoder and decoder for the automatic decoding of the software or data dependent on the stored license parameters; and

an installation for the production of a random secret Private Serial Key (SK) for the encoding of the transmission of the license parameters between said licenser and said licensee.

32. A protective device in accordance with Claim 31, wherein:

the memory includes several memory areas for the storage of license parameters of different licensers.

33. A protective device in accordance with Claim 31 wherein:

the microprocessor, the memory, the encoder/ decoder, and the installation for the production of the Private Serial Key (SK) are developed on a single integrated semiconductor circuit (ASIC).

34. A protective device in accordance with Claim 31 including:

a limiter secure from manipulation that limits the time period and/or the number of decodings of the protected software or data.